Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	**GN Docket No. 13-111**
	)	
	)	

COMMENTS OF SCREENED IMAGES, INC. D.B.A. CORRECTIONS.COM

In its previous Comments, Corrections.com asserted that the FCC should allow for the termination of contraband wireless devices found in correctional facilities. As an addendum to those Comments, Corrections.com has developed the following process, utilizing the CIS data to identify and submit these devices for termination.

This process provides public safety agencies with CIS data that will meet the "clear and convincing" evidentiary standard to obtain a court order requiring the termination of the subscriber account and the disabling of the user equipment. Disabling user equipment by adding these devices to the stolen phone database, or other similar database, will prevent users from establishing new subscriber accounts.

This process enables CIS providers to lessen the burden on public safety agencies, by providing the forensic data and evidence necessary to obtain a court order, while giving the public safety agency the control to guide the process and all

final decision-making authority as to which devices are submitted for termination. It also lessens the burden on the CMRS providers by requiring only limited subscriber data and ensuring that the providers do not incur liability when subscriber accounts are terminated and user equipment disabled.

The steps of this proposed process are as follows:

1 – Public safety agency provides administrative subpoena for all carriers and the MAS provider.

2 – Public safety agency provides warrant for MAS SMS data.

3 – CIS provider Creates 90 Day IMSI/IMEI List. The list includes the following data for each unauthorized device registering on property:

- IMSI and all corresponding IMEI (current and historical)
- IMEI and all corresponding IMSI (current and historical)
- Number of 911 attempts (current and historical)
- Date first seen on CIS (current and historical)
- Date last seen on CIS
- Total # of Captures by CIS (current and historical)
  - Data, SMS, Calls, Registrations
- Destination Numbers (current and historical)
- SMS Contents and SMS Destination Numbers (current and historical)
- Date/time of every interaction with the CIS
  - Data, SMS, Calls, Registrations

4 - CIS provider requests the following information from the DOC:

- Staff List (with addresses and phone numbers)
- Staff Emergency Contact List (with addresses and phone numbers)
- Staff schedule information (hours on property)
- Approved Visitors List (with addresses and phone numbers)
- Visiting Hours (hours visitors on property)
- Approved Inmate Call List
- Inmate Pin List
- Volunteer List (with addresses and phone numbers)
- Volunteer Schedules (hours on property)
- Contractor List (with addresses and phone numbers)
- Contractor Schedules (hours on property)
- Internal Investigation Unit Inmate Gang and Association List

5 – CIS provider requests the following information from all carriers to verify ownership of all unauthorized devices on the 90 Day IMSI/IMEI List:

- Account Owner
- Addresses
- UE Phone Number
- IMSI/ESN, IMEI/MEID, MDN, MIN
- Related IMSI/ESN, IMEI/MEID, MDN, MIN
- Account Start/End Dates (historical)
- Account Status (active, cancelled, suspended)
- Service Types/Features
- Associated Phone Numbers
- Credit Card/Bank Account used to pay for service
- Subscriber Date of Birth
- Subscriber Social Security Number
- Subscriber Driver's License
- Subscriber Contact Info (phone/email)

6 – CIS provider's data analytics software uses a weighted algorithm, which looks at a number of variables to determine whether device is an inmate device or whether it fits into one of three other categories of devices, which are outlined below. Those variables are as follows:

- 911 attempts
  - Number of attempts
  - Date/Time of 911 attempts
  - Legitimate or illegitimate
- Owner of Device
  - Staff
  - Contractor
  - Visitor
  - Inmate
  - False Name
  - Unknown Person
- Date/times seen by the CIS
  - Compare dates/times to facility work hour schedules, visiting hours, volunteer hours, etc.
- Suspicious call attempt destination numbers - look for correlations between:
  - Phone Numbers on Approved Inmate Call List
  - Phone Numbers of Approved Visitors List
  - Phones Numbers on Staff Contact List
  - Phone Numbers on Staff Emergency Contact List
  - Phone Numbers on Facility Contractor List
  - Phone Numbers on Facility Volunteer List
  - Phone Numbers of Other Known Inmate Devices

    - Phone Numbers on Internal Investigations Unit Inmate Gang and Association List
- Suspicious SMS Contents and Destination Numbers
    - Contents:
        - E.g. Is user asking someone to put money on a greendot or jpay account?
        - E.g. Did user provide their name or an inmate number in any SMS?
        - E.g. Did user provide their address in any SMS?
    - Destination Numbers – look for correlations between:
        - Phone Numbers on Approved Inmate Call List
        - Phone Numbers of Approved Visitors List
        - Phones Numbers on Staff Contact List
        - Phone Numbers on Staff Emergency Contact List
        - Phone Numbers on Facility Contractor List
        - Phone Numbers on Facility Volunteer List
        - Phone Numbers of Other Known Inmate Devices
        - Phone Numbers on Internal Investigations Unit Inmate Gang and Association List
- Subscriber account information
    - Account Owner
        - Is this a "known person"? (i.e. someone on one of the facility lists)
        - False Name?
        - Unknown person?
    - Name on bank account/credit card used to pay for service
        - Is this a "known person"? (i.e. someone on one of the facility lists)
        - False name?
        - Unknown person?
    - Look at other subscriber account information.
- Algorithm outlined about parses list of IMSIs and IMEIs into four categories:
    - Inmate Phone
        - Organized by carrier. Recommended for termination
    - Known Persons #1 - seen but no communications
        - Submit list to DOC Internal Investigations Unit to remind users that devices are prohibited on property.
    - Known Persons #2 - no suspicious communications
        - Submit list to DOC Internal Investigations Unit to remind users that devices are prohibited on property.
    - Known Persons #3 - suspicious communications
        - Submit list to DOC Internal Investigations Unit for further investigation.
        - DOC may submit a warrant to the carrier requesting additional information, including but not limited to:

- Call History and Related Accounts
- Call Detail Records: telephone call records, call records, call detail, call history, call activity, all calls to and from, all incoming and outgoing calls, phone records, toll records, billed call records, local and long distance calls, dialed numbers, etc.
- Sector Info
- SMS data

7- CIS provider provides DOC with a list of IMSI/IMEI that is organized into four categories of devices (categories outlined in Step #6 above). DOC may submit a subpoena/warrant to the carrier requesting additional information, including but not limited to:

- Call History and Related Accounts
- Call Detail Records: telephone call records, call records, call detail, call history, call activity, all calls to and from, all incoming and outgoing calls, phone records, toll records, billed call records, local and long distance calls, dialed numbers, etc.
- Sector Info
- SMS data

8 – Public safety agency submits IMSI/IMEI List Inmate Devices to carriers for termination.

9 – CIS provider receives confirmation of termination (or other disposition) and flags IMSIs and IMEIs in database.

10 – Public safety agency may request that CIS provider add certain devices to a "Watch List" (i.e. devices that may be inmate devices but where inmate status has not been proven with certainty at this time).

CONCLUSIONS

Corrections.com urges the FCC to allow for the termination of contraband wireless devices found in correctional facilities through a court ordered process. In this addendum, Corrections.com recommends codifying a process, such as the one outlined above. A codified process will lessen the burden on public safety agencies by providing these agencies with the data to meet the "clear and convincing" evidentiary standard and thus the ability to obtain a court order requiring the termination of these devices. Such a process will ensure that only contraband devices are terminated and will remove the incentive for inmates to continue to purchase wireless devices, ending this black market inside correctional facilities.

Respectfully submitted,

/s/ Joseph S. Noonan

Joseph S. Noonan

CEO

Screened Images, Inc. d.b.a. Corrections.com

Dated: February 7, 2018